Legislative Audit Division

State of Montana

Report to the Legislature

December 2005

Information System Audit

Datacenter Security

Montana Department of Transportation

This report contains recommendations to strengthen datacenter environmental and physical security controls. Controls can be improved by implementing a process to identify and address environmental threats to the datacenter including water, power outages, and natural disasters, eliminating excessive physical access to the datacenter, and defining datacenter physical access security requirements.

Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705

06DP-02

Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee, which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Joe Balyeat, Vice Chair	Representative Dee Brown
Senator John Brueggeman	Representative Hal Jacobson
Senator Jim Elliott	Representative Christine Kaufmann
Senator Dan Harrington	Representative Scott Mendenhall
Senator Lynda Moss	Representative John Musgrove, Chair
Senator Corey Stapleton	Representative Janna Taylor

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel

Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

December 2005

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit over the security of the Montana Department of Transportation's datacenter. Our audit focused on the effectiveness of controls implemented to safeguard the datacenter from physical, environmental, and electronic data access threats.

This report contains recommendations identifying areas where the Montana Department of Transportation can strengthen physical and environmental controls. Controls can be improved by implementing a process to identify and address environmental threats to the datacenter, restricting physical access to the datacenter to only those individuals with a demonstrated need, and defining datacenter physical security access requirements. The department's response to the audit report is contained at the end of the report.

We wish to express our appreciation to the department for their cooperation and assistance.

Respectfully submitted,

/s/ Scott A. Seacat

Scott A. Seacat
Legislative Auditor

Room 160, State Capitol Building PO Box 201705 Helena, MT 59620-1705
Phone (406) 444-3122 FAX (406) 444-9784 E-Mail lad@mt.gov

Legislative Audit Division

Information System Audit

Datacenter Security

Montana Department of Transportation

Members of the audit staff involved in this audit were Jessie Solem, Dale Stout, and Nathan Tobin.

Table of Contents

Appointed and Administrative Officials

Montana Department of Transportation	Jim Lynch, Director
	Jim Currie, Deputy Director
	Dick Clark, Administrator, Information Services Division
	Larry Flynn, Acting Administrator, Information Services Division (Effective 12-19-05)

Executive Summary

The Montana Department of Transportation (MDT) is responsible for serving the public by establishing and maintaining a transportation system that emphasizes safety, environmental preservation, cost-effectiveness, economic vitality, and quality. MDT operates a datacenter that houses approximately $1.2 million of hardware designated to manage data and applications used by MDT to facilitate its business operations. A primary objective of the datacenter is to secure the hardware and information systems where data resides. The security of the datacenter creates the foundation for business continuity by ensuring data and information systems are available.

Information systems residing in the datacenter are used to collect and disburse revenue. During fiscal year 2005, MDT collected approximately $2 million a day in revenue and disbursed approximately $1.5 million in expenditures. Systems residing in the datacenter also provide safety information to the traveling public on road and weather conditions, and assist maintenance crews in maintaining safe driving conditions.

A datacenter must keep high standards for maintaining the integrity and functionality of the computer environment through the implementation of complete and effective security measures. The scope of this audit focused on the effectiveness of controls implemented to safeguard the datacenter from physical, environmental, and logical threats. Audit work included interviews and observations with MDT personnel to confirm: physical access points to the datacenter are secure, unrestricted physical access to datacenter resources is prevented, the existence and proper operation of environmental safeguards (i.e. fire suppression/detection systems, backup power supplies, etc.) and datacenter hardware is maintained. Review of entry logs and cardholder reports was conducted to confirm individual physical access to the datacenter is authorized and individual accountability is maintained when accessing the datacenter. Documentation review and an automated network assessment tool were used to confirm logical access to datacenter resources is limited to authorized users.

Executive Summary

Based on our work, we determined that logical access controls limit access to datacenter resources to authorized users. While MDT has implemented environmental and physical safeguards, controls can be strengthen by implementing a process to identify and address environmental threats to the datacenter including water, power outages, and natural disasters, eliminating excessive physical access to the datacenter, and defining datacenter physical access security requirements

Chapter I - Introduction and Background

Introduction and Background

The Montana Department of Transportation (MDT) is responsible for serving the public by establishing and maintaining a transportation system that emphasizes safety, environmental preservation, cost-effectiveness, economic vitality, and quality. MDT operates a datacenter that houses approximately $1.2 million of hardware designated to manage data and applications used by MDT to facilitate its business operations. A primary objective of the datacenter is to secure the hardware and information systems where data resides. The security of the datacenter creates the foundation for business continuity by ensuring data and information systems are available.

Information systems residing in the datacenter are used to collect and disburse revenue. During fiscal year 2005, MDT collected approximately $2 million a day in revenue and disbursed approximately $1.5 million in expenditures. In addition to funds distribution and collection, systems residing in the datacenter also provide safety information to the traveling public on road and weather conditions, and assist maintenance crews in maintaining safe driving conditions. Weak datacenter security controls could disrupt the availability of data and result in a delay of revenue collection and disbursement of expenditures, as well as affect the safety of the traveling public.

Audit Objectives

A datacenter must keep high standards for maintaining the integrity and functionality of the computer environment through the implementation of complete and effective security measures. To determine what security measures MDT has in place to protect the datacenter and maintain its business operations, we conducted an audit of the datacenter security to meet the following objectives.

- **Determine whether physical access controls over the datacenter adequately safeguard against physical threats.** Physical security involves restricting physical access to computer resources, usually by limiting access to the buildings and rooms where they are housed, or by installing locks on computer terminals.

- **Determine whether environmental controls over the datacenter adequately safeguard against environmental threats.** Environmental controls prevent or mitigate potential damage to facilities and interruptions in service caused by unexpected disruptive events (i.e. fire, flood, loss of power, temperature fluctuations, etc.).
- **Determine whether logical access controls over the datacenter adequately safeguard against logical threats.** Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers, passwords or other identifiers that are linked to predetermined access privileges.

Audit Scope and Methodology

The audit was conducted in accordance with Government Auditing Standards published by the United States General Accountability Office (GAO). We evaluated the control environment using state law, MDT policy, and generally applicable and accepted information technology standards established by the IT Governance Institute and the computer security incident response team CERT®.

The scope of this audit is limited to the physical, environmental, and logical access controls over the MDT datacenter. The scope did not include applications and hardware external to the datacenter or logical access security to individual servers residing inside the datacenter.

Audit work included interviews and observations with MDT personnel to confirm: physical access points to the datacenter are secure, unrestricted physical access to datacenter resources is prevented, the existence and proper operation of environmental safeguards (i.e. fire suppression/detection systems, backup power supplies, etc.) and datacenter hardware is maintained. Review of entry logs and cardholder reports was conducted to confirm individual physical access to the datacenter is authorized and individual accountability is maintained when accessing the datacenter. Documentation review and an automated network assessment tool were used to confirm logical access to datacenter resources is limited to authorized users.

Management Memo

During the course of the audit, we identified one issue regarding the configuration of the temperature monitoring controls installed on datacenter hardware. The temperature monitoring controls are provided by the hardware vendor and are delivered with default operating temperature ranges; however, the vendor recommends configuring the temperature range considering the elevation in which the hardware will operate. The temperature monitoring devices installed on the datacenter hardware retain the default temperature setting and the elevation of Helena has not been considered. We believe this issue warrants management attention; however, this issue was not included as a recommendation in this report, but was discussed with the Montana Department of Transportation.

Conclusion

Protection of datacenter hardware is provided through the existence and operation of logical, physical, and environmental controls. We confirmed that logical access controls limit access to datacenter resources to authorized users. We determined MDT can strengthen environmental and physical controls to ensure datacenter resources are safeguarded.

MDT acknowledged in its 2004 strategic information technology (IT) plan that it is not properly prepared for IT disasters and recognized the need to begin developing plans to address disaster recovery processes. Therefore, at this time there are no recommendations to address disaster recovery plans. In light of the issues MDT has acknowledged exist, MDT can strengthen environmental controls by implementing a process to identify and address datacenter environmental threats that could disrupt MDT business operations.

Physical security depends on controls implemented to restrict physical access to datacenter resources. Physical controls can be improved by defining physical security requirements related specifically to the datacenter, and ensuring physical access to the datacenter is limited to only those individuals who require the access.

Chapter II - Environmental Security Controls

Environmental Security Introduction

Environmental controls prevent or mitigate potential damage to facilities and interruptions in service caused by unexpected disruptive events (i.e. fire, flood, loss of power, temperature fluctuations, etc.). Environmental controls can diminish losses from some interruptions or prevent incidents by detecting potential problems early. Implementation of environmental controls are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters.

Environmental Security Conclusion

Based on our work, MDT can strengthen environmental security controls by conducting an assessment to identify and address threats to the datacenter environment caused by the presence of food and beverages, lack of emergency lighting, location of hardware primary and secondary power supplies, and a natural disaster rendering the datacenter physically inaccessible. The following sections discuss these vulnerabilities.

No Assessment of Environmental Threats

The existence of unaddressed environmental threats within the datacenter could affect the operation of hardware residing in the datacenter and disrupt MDT business operations. MDT has demonstrated consideration for environmental risks within the datacenter through the implementation of safeguards such as fire detection and suppression devices, water detection devices, secondary power supplies to datacenter hardware, and temperature control and monitoring devices. However, MDT has not conducted an assessment to identify the range of environmental risks to the datacenter, and vulnerabilities exist that could disrupt MDT's business operations.

No Food and Beverage Restrictions

MDT has not restricted personnel from bringing food or beverages into the datacenter. Industry best practices recommend prohibiting eating and drinking within computer facilities. In a computing environment, the presence of food and beverage creates the risk for spills and damage to hardware. MDT management stated that personnel understand the risk associated with bringing food and drink into the datacenter and this understanding will prevent

incidents. However, each piece of equipment in the datacenter is worth between $1,000 and $300,000 and damage to any one piece could be costly. Restricting food and beverage in the datacenter is an inexpensive way to prevent what could be a costly accident.

No Emergency Lighting

In the event of a power outage, the datacenter is without lighting. MDT has implemented secondary power sources to maintain the operations of a majority of the datacenter's equipment during power outages; however, there is not a secondary power source for the lighting system in the datacenter. In addition, due to the location of the datacenter, no windows are present to provide natural lighting. As a result, an outage of the primary power source will leave the datacenter in the dark and the completion of day-to-day activities required to keep the datacenter fully operational may be difficult to complete due to a lack of visibility. MDT staff stated that during past power outages, a flashlight has been used to access the datacenter.

Inadequate Business Continuity Preparedness

Montana is one of the most seismically active states in the United States, and an earthquake poses one of the largest natural disaster threats to the state. Montana's earthquake activity is concentrated mostly in the mountainous western region. The city of Helena experienced a series of earthquakes in October of 1935 that reached a magnitude of 6.3. According to Montana's Disaster and Emergency Services, in the Helena region the return time for an earthquake of a 6+ magnitude is approximately 70 years. Montana has experienced major earthquakes in the past and there is reason to believe that similar events will occur. MDT has not implemented controls to ensure business continuity in the event an earthquake renders the datacenter physically inaccessible.

MDT has demonstrated consideration for disaster recovery as illustrated through its September 2003 draft disaster recovery plan outlining recovery steps, off-site storage of data backup files, and restoration of datacenter operations within 72 hours through a vendor contract.

However, each of these disaster recovery considerations depend on the existence and accessibility of the datacenter. The datacenter is located at the lowest point of the MDT building and in the event of a disastrous earthquake the datacenter may be inaccessible. MDT's draft disaster recovery plan does not address recovery in the event the datacenter is physically inaccessible and without access to the datacenter, datacenter operations cannot be restored. While MDT maintains backup files of its data stored at off-site locations, without access to the hardware to make the data accessible and available, MDT cannot ensure business continuity. In MDT's 2004 strategic IT plan, MDT recognized a lack of an appropriate disaster recovery plan and preparedness in the event of IT disasters. MDT further acknowledged that they are not in compliance with state IT standards regarding disaster recovery plans and recognized the need to begin developing plans to address disaster recovery processes.

Unprotected Power Supply

The datacenter is located at the lowest point of the MDT building and is in close proximity to the building's water supply. Damaged water lines and pipes could lead to drainage and water accumulation. Because the datacenter is at the lowest point in the building, water accumulation could damage equipment and disrupt MDT business operation. To mitigate the risk created by water, datacenter hardware is stored on floors elevated 12 inches off the ground. According to MDT personnel, when the datacenter was first designed, raised floors were implemented to store electrical wiring to prevent hazards caused by multiple wiring cables arranged on the floor. Subsequently, the primary and secondary power supplies, as well as the electrical outlets, to the hardware are stored beneath the raised floor, directly on the ground. Water accumulation could damage the electrical wiring and outlets supplying power to the hardware, resulting in loss of power and hardware operation.

Summary

MDT has not conducted an assessment to identify the complete range of risks present in the datacenter environment, therefore, decisions have not been made regarding how the risks should be managed to an acceptable level. MDT has demonstrated consideration of environmental threats through the implementation

of safeguards such as fire suppression and detection devices and has not considered the possibility that unaddressed threats are present in the datacenter environment. Implementation of a process to periodically assess and address vulnerabilities could mitigate threats to datacenter hardware and disruptions to MDT's business operations.

Recommendation #1

We recommend the department implement a process to identify and manage environmental threats to the datacenter.

Chapter III - Physical Security Controls

Physical Security Introduction

Physical security controls restrict physical access to IT resources by limiting access to the building and rooms where resources are housed. MDT uses an electronic card key access control system with magnetic doors to protect datacenter resources from loss or impairment due to intentional or unintentional human interaction. Access is limited to individuals who have been assigned a card key.

Physical Security Conclusion

Based on our work, physical security controls can be improved by defining and documenting physical security requirements and procedures specific to the datacenter, and ensuring physical access to the datacenter is limited to only those individuals who require the access. The following sections discuss these vulnerabilities.

Undocumented Datacenter Physical Access Requirements

The Facilities Bureau of the Maintenance Division is responsible for centrally administering card key access to the MDT headquarters building, including the datacenter secured doors. MDT has implemented a card entry policy to administer employee card key access to the headquarters building. Access to the headquarters building is provided to all employees; however, within the building there are rooms that contain specialized equipment, such as the datacenter, and physical access is selectively granted and not provided universally to all employees. The card entry policy does not define physical access requirements to the datacenter such as who should have access, how physical access is requested, and who can approve physical access requests.

During the audit, we determined that 25 individuals have physical access privileges to the datacenter. We reviewed these individuals to determine if: 1) a completed card entry form existed, 2) the card entry form was approved, 3) datacenter access was requested, and 4) the employee was active.

Terminated Employee

When an employee terminates, the employee's supervisor is responsible for collecting the employee's card key to deactivate physical access privileges. We determined one of the 25 individuals with datacenter physical access retained access after their

termination date. MDT management stated that they try to ensure all terminated employees' access is revoked upon termination; however, collection of this employee's card key and subsequent deactivation of their physical access rights was overlooked. We reviewed a report of the terminated employee's card key's use and determined the employee did not physically access the datacenter after their termination date. Upon our notification of the terminated employee, MDT personnel deactivated the employee's physical access.

No Evidence of Datacenter Access Request

In order to obtain physical access to the MDT headquarters building, an employee must complete a card entry form. Access to the datacenter can only be obtained if the employee also has physical access to the MDT headquarters building. Thus, all employees with datacenter access should have a completed card entry form. An informal understanding exists to request physical access to the datacenter in the comments section of the card entry form.

We determined four of the 25 individuals with access did not complete a card entry form. Of the 21 individuals with a completed card entry form, twelve did not request datacenter access on the form. As a result, no evidence is available to substantiate that requests for physical access to the datacenter were made for 16 individuals. MDT management determined one of these individuals did not require physical access to the datacenter and their access was deactivated.

MDT management believes awareness of the card entry policy is not widespread amongst MDT employees and personnel responsible for granting requested physical access. Furthermore, MDT's current card entry policy and form do not specifically address the datacenter and how physical access should be requested. During the audit, MDT personnel redesigned the card entry form to include an area to request datacenter access and required all employees to complete and resubmit the new form. MDT management plans to inform employees of the new form through MDT's bi-weekly newsletter and include a link to the card entry policy to facilitate awareness of the policy.

No Authorization of Physical Access

According to Information Services Division (ISD) personnel who are responsible for physical security of the datacenter, datacenter access requests should be approved at the bureau chief level. We reviewed the card entry form for individuals with datacenter access to determine if the access was approved and authorized by a bureau chief. We determined that of the 21 individuals with completed card entry forms, two individuals lacked authorizing signatures and four individual's datacenter access requests were not authorized by a bureau chief. Consequently, there is no evidence to substantiate that these six individuals have been authorized physical access to the datacenter. MDT management stated that in the past physical access has been granted through verbal request or e-mails. In addition, the prior ISD bureau chief informally designated two supervisors within ISD the authority to approve datacenter access requests and the designation was not documented. ISD currently has no documented policy in place regarding who has the authority to authorize physical access to the datacenter so access is informally authorized.

Excessive Physical Access

ISD is responsible for physically securing the datacenter; however, ISD exercises no control over maintenance employees' access to the datacenter. ISD has not defined Maintenance Division duties that require physical access to the datacenter and maintenance employees' physical access requests to the datacenter are authorized by the Facilities Bureau's bureau chief.

We reviewed individuals with datacenter physical access and determined that physical access is provided to individuals who do not require the access to perform their duties. Ten employees of the Maintenance Division have physical access to the datacenter; however, upon discussion with MDT management, we determined that only three of the ten maintenance employees require physical access to the datacenter to perform maintenance functionality. MDT management stated that prior to the implementation of the new air conditioning system during the summer of 2005, a stand-alone unit located within the datacenter provided cooling. This unit's operability was not reliable and maintenance employees were provided physical access to the datacenter to perform daily

maintenance and monitoring. The new air conditioning system is external to the datacenter and MDT management stated maintenance employees' physical access to the datacenter should be reassessed and guidelines established to define who should be provided datacenter physical access.

Summary

MDT has implemented a card entry policy to administer card key access to the headquarters building; however, the procedures defined in the policy do not address physical access management of the datacenter. As the responsible party for datacenter physical security, ISD needs to take ownership of datacenter security and define requirements to ensure physical access to the datacenter is documented, authorized by formally designated personnel, and limited to current and appropriate employees.

Recommendation #2

We recommend the department:

A. Define, document, and implement a policy to address physical security requirements and procedures specific to the datacenter.

B. Evaluate physical access to the datacenter and remove all unnecessary access.

Department Response

Montana Department of Transportation
2701 Prospect Avenue
PO Box 201001
Helena MT 59620-1001

Jim Lynch, Director
Brian Schweitzer, Governor

November 30, 2005

Jessie Solem
Legislative Audit Division
PO Box 201705
Helena, MT 59620-1705

Subject: Datacenter security audit

Dear Jessie,

We have reviewed the Legislative Audit Division's Datacenter Security Audit and the recommendations contained therein. Our response to your recommendations appear below:

Recommendation 1

We recommend the department implement a process to identify and manage environmental threats to the datacenter.

Response

We concur. The department recognizes the need to address environmental threats to the datacenter. Recently, the Information Services Division has created a new disaster recovery position to directly deal with these issues. This position has been filled and the successful candidate will begin in December 2005.

Among the duties of this new position will be the development and implementation of a comprehensive disaster recovery plan addressing the environmental threats to the datacenter. This will include a thorough assessment of the environmental risks to the datacenter and implementation of policy and procedures to mitigate these risks. The department intends to have this disaster recovery plan developed by the end of the current fiscal year and implementation of the plan to commence immediately thereafter as resources allow.

MDT has already taken steps to begin mitigating the environmental threats to the datacenter. Signs have been posted throughout the facility prohibiting food and beverages within the datacenter. Further, the Facility Bureau has begun investigating alternatives to addressing and mitigating other environmental risks associated with the datacenter.

Recommendation 2

We recommend the department:

Director's Office
Phone: (406) 444-6201
Fax: (406) 444-7643

Web Page: www.mdt.mt.gov
Road Report: (800) 226-7623 or 511
TTY: (800) 335-7592

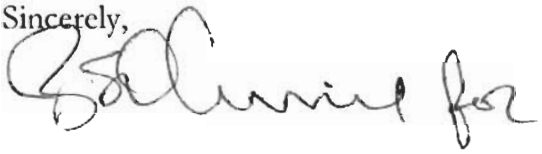
A. Define, document, and implement a policy to address physical security requirements and procedures specific to the datacenter.
B. Evaluate physical access to the datacenter and remove all unnecessary access.

Response
Again, we agree. The department will define, document, and implement a comprehensive policy to address all aspects of the physical security of the datacenter. The Information Services Division and the Facilities Bureau of the Maintenance Division will work jointly to develop and implement these policies. The department intends to have this policy fully developed and implemented by the end of the third quarter of this fiscal year.

Additionally, the department will immediately evaluate those individuals who currently have access to the datacenter and to remove access to those deemed unnecessary. This will be completed by the end of December 2005.

Jessie, thank you for the friendly and professional manner in which you and your staff conducted this audit. We look forward to working with you in the future.

Sincerely,



Jim Lynch
Director

copies: Dick Clark, ISD Administrator
John Blacker, Maintenance Administrator